

Exact Analytical Bit Error Rates for Multiple Access Chaos-Based Communication Systems

Wai M. Tam, Francis C. M. Lau, *Senior Member, IEEE*, Chi K. Tse, *Senior Member, IEEE*, and Anthony J. Lawrance

Abstract—In this paper, exact analytical expressions for the bit error rates (BERs) in a multiple-access chaos-based digital communication system are derived. Comparisons are made with those obtained using traditional approximation methods which assume a Gaussian distribution for the conditional decision parameter. The obtained results are compared to the results of brute-force (BF) numerical simulations. It is found that the exact analytical BERs are in perfect agreement with BF simulations and hence provide better prediction of the BER performance than those given by traditional Gaussian-approximation-based methods.

Index Terms—Chaos-based communications, exact bit error rate (BER), multiple access.

I. INTRODUCTION

ONE POTENTIAL application of chaos in engineering is the spreading of spectrum for telecommunications since chaotic signals are inherently wideband and their generation is relatively inexpensive. Chaos-based communication systems in digital forms have been found feasible for practical realization, and a number of chaos-based digital communication systems have been proposed in the past, e.g., the chaos-shift-keying system [1] and the differential chaos-shift-keying system [2]. Being spread-spectrum systems occupying bandwidths much wider than what their information contents require, chaos-based communication systems are expected to provide multiple access and consequently their performance should be evaluated under a multiple access environment [3]–[5]. Of particular concern to communication engineers is the prediction of the bit error performance of these systems under additive white Gaussian noise (AWGN) conditions. Traditional methods for calculating the bit error rate (BER) for a given chaos-based communication system are based on the assumption of a Gaussian distribution of the conditional decision parameter concerned [6]. The resulting BERs are inexact and may in some cases deviate significantly from the actual BERs computed from brute-force (BF) numerical simulations. In this paper, we apply an exact analytical method, which was proposed by Lawrance and Ohama

[7], to derive expressions for the BERs in a multiple access chaos-based digital communication system. We compare the results with those obtained from traditional methods based on the assumption of Gaussian distributed decision parameter, the control being provided by BF numerical simulations. The results reveal that the exact analysis can provide very accurate prediction of BERs even for small spreading factors, whereas the traditional Gaussian-approximation (GA) based method gives only good approximation when the spreading factor is large.

II. SYSTEM DESCRIPTION

The system under study is an antipodal coherent chaos-shift-keying (CSK) communication system with N users, and we consider the discrete-time baseband equivalent model shown in Fig. 1. Suppose the i th user is transmitting a binary symbol $d_l^{(i)}$ during the l th-bit duration, and the symbol $d_l^{(i)}$ is either “+1” or “−1,” each with a probability of 1/2. Also, the symbols sent by different users are independent of one another. The CSK modulation process is applied here to spread the binary symbol sequences. Essentially, there are N chaos generators corresponding to the N different users, and the i th chaos generator produces the chaotic samples $\{x_k^{(i)}\}$, which is used to spread the binary symbol sequence $\{d_l^{(i)}\}$ during the l th bit duration. We also assume that the chaotic samples $\{x_k^{(i)}\}$ are obtained by repeating a truncated, long chaotic signal [8], [9], which is made known at the receiver side. Let β be the spreading factor, which is simply the number of chaos samples transmitted in one bit duration. The signal transmitted by user i at time $k = (l-1)\beta + 1, (l-1)\beta + 2, \dots, l\beta$, under the antipodal CSK scheme, can be written as

$$s_k^{(i)} = d_l^{(i)} x_k^{(i)}. \quad (1)$$

Assuming that the users are chip synchronized, the overall transmitted signal of the system at time k is thus given by

$$s_k = \sum_{i=1}^N s_k^{(i)}. \quad (2)$$

We assume that the chaotic sequences are generated independently of one another. Also, the mean value of each chaotic sequence is necessarily zero in order to avoid transmitting any noninformation-bearing dc components, i.e.,

$$E[x_k^{(i)}] = 0, \quad i = 1, 2, \dots, N \quad (3)$$

where $E[\psi]$ denotes the mean value of ψ .

Manuscript received February 26, 2003; revised July 28, 2003 and October 28, 2003. This work was supported in part by the Hong Kong Polytechnic University under Research Grant A-PD65, in part by the Hong Kong Research Grants Council under Grant PolyU 5137/02E, in part by the U.K. Engineering and Physical Sciences Research Council (EPSRC) and in part by QinetiQ (Malvern). This paper was recommended by Associate Editor L. Kocarev.

W. M. Tam, F. C. M. Lau, and C. K. Tse are with the Department of Electronic and Information Engineering, the Hong Kong Polytechnic University, Hong Kong (e-mail: tamwm@eie.polyu.edu.hk; encmlau@polyu.edu.hk; encktse@polyu.edu.hk).

A. J. Lawrance is with the School of Mathematics and Statistics, Birmingham University, Birmingham B15 2TT, U.K. (e-mail: A.J.Lawrance@bham.ac.uk).

Digital Object Identifier 10.1109/TCSII.2004.832773

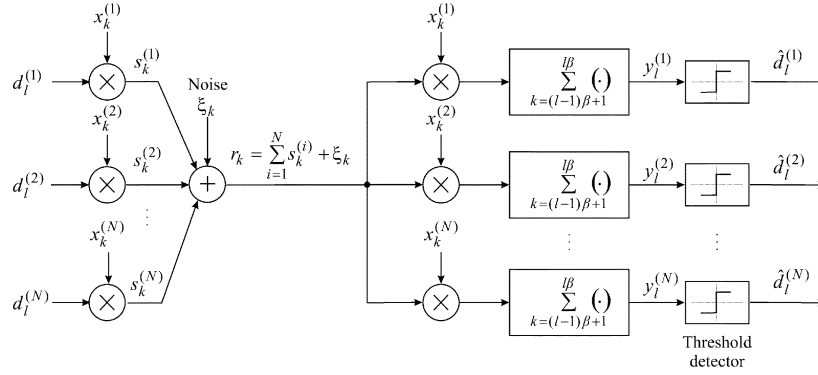


Fig. 1. Multiple access chaos-based communication system.

As the signal goes through a communication channel, noise is being added. For an AWGN channel, the received signal is given by

$$r_k = \sum_{i=1}^N s_k^{(i)} + \xi_k \quad (4)$$

where ξ_k is an AWGN sample with zero mean and variance $N_0/2$. At the receiving side, the repeated, truncated chaotic spreading signal $\{x_k^{(i)}\}$ is reproduced. Synchronization between the incoming signal and the local chaotic spreading signal can then be achieved by using an integrate-and-dump stage and a threshold detector [8]. As shown in Fig. 1, the receiver basically employs a direct correlation process for demodulation. For the j th user, the output of the correlator, denoted by $y_l^{(j)}$, is given by

$$\begin{aligned} y_l^{(j)} &= \sum_{k=(l-1)\beta+1}^{l\beta} r_k x_k^{(j)} = \sum_{k=(l-1)\beta+1}^{l\beta} \left(\sum_{i=1}^N s_k^{(i)} + \xi_k \right) x_k^{(j)} \\ &= \sum_{i=1}^N d_l^{(i)} \sum_{k=(l-1)\beta+1}^{l\beta} x_k^{(i)} x_k^{(j)} + \sum_{k=(l-1)\beta+1}^{l\beta} \xi_k x_k^{(j)}. \end{aligned} \quad (5)$$

The decision parameter is the correlator output $y_l^{(j)}$ and the recovered symbol, denoted by $\hat{d}_l^{(j)}$, is given by

$$\hat{d}_l^{(j)} = \text{sgn}[y_l^{(j)}] \quad (6)$$

where $\text{sgn}[\cdot]$ is the sign function. The above decoding rule simply says that for the j th user, the recovered symbol is a “+1” if $y_l^{(j)} > 0$, and is a “−1” otherwise.

III. PERFORMANCE ANALYSIS

In this section, we present two approaches for calculating the BERs for the afore-described system. The conventional method assuming Gaussian distribution of the conditional decision parameter $y_l^{(j)}$ with its first two moments is first discussed. We will highlight the main assumption of the method, which may lead to inaccurate performance prediction for some cases. An alternative approach which reaches into the dynamics of the decision parameter is then described. This approach gives exact analytical formulas for the required BERs.

A. Derivation of BERs Based on Gaussian Approximation

With no loss of generality, let us consider the j th user and derive the probability of error for the first symbol. For brevity, we omit the subscript l (which is 1 in this case) in the variables $d_l^{(j)}$, $\hat{d}_l^{(j)}$ and $y_l^{(j)}$. The decision parameter for the j th user is given by

$$y^{(j)} = d^{(j)} \sum_{k=1}^{\beta} (x_k^{(j)})^2 + \sum_{i=1, i \neq j}^N d^{(i)} \sum_{k=1}^{\beta} x_k^{(i)} x_k^{(j)} + \sum_{k=1}^{\beta} \xi_k x_k^{(j)} \quad (7)$$

where the conditioning is only on $d^{(j)}$ and not the others. With a Gaussian distribution assumed for the conditional decision parameter, the BER for user j can then be evaluated by

$$\begin{aligned} \text{BER}^{(j)} &= \frac{1}{2} \text{Prob}(y^{(j)} \leq 0 \mid d^{(j)} = +1) \\ &\quad + \frac{1}{2} \text{Prob}(y^{(j)} > 0 \mid d^{(j)} = -1) \end{aligned} \quad (8)$$

where the two conditional error probabilities are approximated by

$$\begin{aligned} \text{Prob}(y^{(j)} \leq 0 \mid d^{(j)} = +1) &= \frac{1}{2} \text{erfc} \left(\frac{E[y^{(j)} \mid d^{(j)} = +1]}{\sqrt{2 \text{var}[y^{(j)} \mid d^{(j)} = +1]}} \right) \\ \text{Prob}(y^{(j)} > 0 \mid d^{(j)} = -1) &= \frac{1}{2} \text{erfc} \left(\frac{-E[y^{(j)} \mid d^{(j)} = -1]}{\sqrt{2 \text{var}[y^{(j)} \mid d^{(j)} = -1]}} \right). \end{aligned} \quad (9)$$

In (9) and (10), $\text{var}[\cdot]$ represents the variance operator and $\text{erfc}(\cdot)$ denotes the complementary error function defined as

$$\text{erfc}(\psi) \equiv \frac{2}{\sqrt{\pi}} \int_{\psi}^{\infty} \exp(-t^2) dt. \quad (11)$$

Suppose the j th user is sending a “+1.” The mean value of $y^{(j)} \mid d^{(j)} = +1$ is given by

$$E[y^{(j)} \mid d^{(j)} = +1] = \beta E[(x_k^{(j)})^2]. \quad (12)$$

Also, from the independence of the chaotic sequences, the variance of $y^{(j)} | d^{(j)} = +1$ is readily shown equal to

$$\begin{aligned} \text{var} [y^{(j)} | d^{(j)} = +1] &= \beta \text{var} [(x_k^{(j)})^2] + \sum_{k=1}^{\beta} \sum_{m=1, m \neq k}^{\beta} \text{cov} [(x_k^{(j)})^2, (x_m^{(j)})^2] \\ &\quad + \beta E [(x_k^{(j)})^2] \sum_{i=1, i \neq j}^N E [(x_k^{(i)})^2] \\ &\quad + \sum_{i=1, i \neq j}^N \sum_{k=1}^{\beta} \sum_{m=1, m \neq k}^{\beta} E [x_k^{(i)} x_m^{(i)}] E [x_k^{(j)} x_m^{(j)}] \\ &\quad + \frac{1}{2} \beta N_0 E [(x_k^{(j)})^2]. \end{aligned} \quad (13)$$

Notice that in the derivation of the mean and variance of $y^{(j)} | d^{(j)} = +1$, the expectation is taken over both the x 's and the other d 's except $d^{(j)}$. Now, using

$$E [y^{(j)} | d^{(j)} = -1] = -E [y^{(j)} | d^{(j)} = +1] \quad (14)$$

$$\text{var} [y^{(j)} | d^{(j)} = -1] = \text{var} [y^{(j)} | d^{(j)} = +1] \quad (15)$$

it is seen that the two conditional probabilities in (9) and (10) are equal, and the BER for user j is simplified to

$$\begin{aligned} \text{BER}^{(j)} &= \text{Prob} (y^{(j)} \leq 0 | d^{(j)} = +1) \\ &= \frac{1}{2} \text{erfc} \left(\frac{E [y^{(j)} | d^{(j)} = +1]}{\sqrt{2 \text{var} [y^{(j)} | d^{(j)} = +1]}} \right). \end{aligned} \quad (16)$$

Clearly, the accuracy of the above formulas is subject to the validity of the Gaussian distribution assumption and its moments capturing the exact probabilities. Notice that only low-order moments of the chaotic spreading sequences have been considered, which are not enough to characterize them. Thus, the formulas could give identical results for quite distinct chaotic spreading. This is the case for Chebyshev spreading with different orders, as will be demonstrated in Section IV. When the spreading factor is sufficiently large, it gives reasonably good estimates of the BERs, but when the spreading factor is small and the distribution of the conditional decision parameter deviates significantly from the Gaussian, the above formulas give rather disappointing results.

Application Example: Suppose the Chebyshev map is used to generate the chaotic signals [10]. In order to provide each user a different chaotic signal, we may either use one Chebyshev map with N different initial conditions or use N Chebyshev maps of different degrees. In either case, the second and fourth terms in (13) can be eliminated since the chaotic signals generated by Chebyshev maps satisfy the following conditions (see Appendix):

$$\text{cov} [(x_k^{(j)})^2, (x_m^{(j)})^2] = 0, \quad k \neq m \quad (17)$$

$$E [x_k^{(j)}, x_m^{(j)}] = 0, \quad k \neq m. \quad (18)$$

Also $E [(x_k^{(i)})^2] = P_s$ for all i , indicating that all users are transmitting with the same average power. The variance of $y^{(j)} | d^{(j)} = +1$ can then be shown equal to

$$\begin{aligned} \text{var} [y^{(j)} | d^{(j)} = +1] &= \beta \text{var} [(x_k^{(j)})^2] \\ &\quad + (N-1) \beta P_s^2 + \frac{1}{2} \beta N_0 P_s. \end{aligned} \quad (19)$$

Writing

$$\Omega = \frac{\text{var} [(x_k^{(1)})^2]}{P_s^2} = \frac{\text{var} [(x_k^{(2)})^2]}{P_s^2} = \dots = \frac{\text{var} [(x_k^{(N)})^2]}{P_s^2} \quad (20)$$

we have the BER for user j given by

$$\text{BER}^{(j)} = \frac{1}{2} \text{erfc} \left(\left[\frac{2\Omega}{\beta} + \frac{2(N-1)}{\beta} + \left(\frac{E_b}{N_0} \right)^{-1} \right]^{-1/2} \right) \quad (21)$$

where E_b denotes the average bit energy and equals βP_s .

B. Derivation of Exact BERs

In this section, we apply the approach of Lawrance and Ohama [7], which gave exact BERs for single-user CSK systems to derive exact analytical results for BERs in multiple-access CSK systems. This approach enables full dynamics of the chaotic spreading to be utilized and not just low order moments of the spreading. First, an exact Gaussian mean and variance result is available for $\text{BER}^{(j)}$ when considered conditionally on the spreading and on the bits of the other users; this follows only from the Gaussian distribution of the noise. Secondly, the full dynamics of the spreading are used to uncondition the result and hence obtain the fully exact $\text{BER}^{(j)}$; this is explicitly obtained as an N -dimensional integral over the independent invariant distributions of the chaotic spreading.

To simplify the notations, we denote the vector of the symbols sent by Users $1, 2, \dots, j-1, j+1, \dots, N$ by $\check{\mathbf{d}}$ and the initial conditions of the unmodulated chaotic signals by the vector \mathbf{X} , i.e.,

$$\check{\mathbf{d}} = [d^{(1)} \ d^{(2)} \ \dots \ d^{(j-1)} \ d^{(j+1)} \ \dots \ d^{(N)}]^T \quad (22)$$

$$\mathbf{X} = [x_1^{(1)} \ x_1^{(2)} \ \dots \ x_1^{(N)}]^T. \quad (23)$$

Given the vectors $\check{\mathbf{d}}$ and \mathbf{X} , the value of $y^{(j)}$ in (7), which is now conditioned on all spreading and transmissions of all other users, has a Gaussian distribution exactly. The mean of the conditional decision parameter, $y^{(j)} | (d^{(j)}, \check{\mathbf{d}}, \mathbf{X})$ can be written as

$$\begin{aligned} E [y^{(j)} | (d^{(j)}, \check{\mathbf{d}}, \mathbf{X})] &= d^{(j)} \sum_{k=1}^{\beta} (x_k^{(j)})^2 + \sum_{i=1, i \neq j}^N d^{(i)} \sum_{k=1}^{\beta} x_k^{(i)} x_k^{(j)}. \end{aligned} \quad (24)$$

Also, because the chaotic sequences are independent, the variance of the decision parameter is readily shown equal to

$$\text{var} [y^{(j)} | (d^{(j)}, \check{\mathbf{d}}, \mathbf{X})] = \text{var} \left[\sum_{k=1}^{\beta} \xi_k x_k^{(j)} \right] = \frac{N_0}{2} \sum_{k=1}^{\beta} (x_k^{(j)})^2. \quad (25)$$

Since $d^{(i)}$ and $x_k^{(i)}$ are independent for all i , the BER for the j th user, $\text{BER}^{(j)}$, can be written as (26) at the bottom of the page, where $h(\mathbf{X})$ denotes the joint probability density function of \mathbf{X} . Using

$$E[y^{(j)} | (d^{(j)} = -1, -\check{\mathbf{d}}, \mathbf{X})] = -E[y^{(j)} | (d^{(j)} = +1, \check{\mathbf{d}}, \mathbf{X})] \quad (27)$$

and

$$\begin{aligned} \text{var}[y^{(j)} | (d^{(j)} = -1, -\check{\mathbf{d}}, \mathbf{X})] \\ = \text{var}[y^{(j)} | (d^{(j)} = +1, \check{\mathbf{d}}, \mathbf{X})] \end{aligned} \quad (28)$$

the $\text{BER}^{(j)}$ given in (26) can be simplified to (29) at the bottom of the page. Since $x_1^{(i)}$'s are independent variables, $h(\mathbf{X})$ is equal to

$$h(\mathbf{X}) = h_1(x_1^{(1)}) \times h_2(x_1^{(2)}) \cdots \times h_N(x_1^{(N)}) \quad (30)$$

where $h_i(x_1^{(i)})$ represents the natural invariant probability density function of $x_1^{(i)}$. Thus, the desired exact result equals (31) at the bottom of the page. This result consists of 2^{N-1} N -dimensional integrals which are numerically explicit, although they may not be computationally practical for large N (how large

being dependent on the numerical software used). The result could also be used to enable the lower limits of accuracy of the moment-based analytical results to be ascertained by comparison.

Based on (24), (25), and (31), it can be seen that to minimize the BER of the j th user, the chaotic sequences $\{x_k^{(i)}\}, i = 1, 2, \dots, N$, should be chosen such that the correlation between any two different chaotic segments of length β , i.e., $\sum_{k=m}^{m+\beta-1} x_k^{(i)} x_k^{(j)}$ with arbitrary m and for $i \neq j$, is very low. Ideally, the two chaotic segments are orthogonal, i.e., $\sum_{k=m}^{m+\beta-1} x_k^{(i)} x_k^{(j)} = 0$ for $i \neq j$. Under such circumstances, (24) is simplified to

$$E[y^{(j)} | (d^{(j)}, \check{\mathbf{d}}, \mathbf{X})] = d^{(j)} \sum_{k=1}^{\beta} (x_k^{(j)})^2. \quad (32)$$

In consequence, (31) becomes (33) shown at the bottom of the next page. For a particular initial condition of the chaotic signal $x_1^{(j)}$ in a bit, the corresponding bit energy equals

$$E_b = \sum_{k=1}^{\beta} (x_k^{(j)})^2. \quad (34)$$

$$\begin{aligned} \text{BER}^{(j)} &= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \sum_{\check{\mathbf{d}}} \left[\text{Prob}(y^{(j)} \leq 0 | (d^{(j)} = +1, \check{\mathbf{d}}, \mathbf{X})) \times \text{Prob}(d^{(j)} = +1) \times \text{Prob}(\check{\mathbf{d}}) \times h(\mathbf{X}) \right. \\ &\quad \left. + \text{Prob}(y^{(j)} > 0 | (d^{(j)} = -1, \check{\mathbf{d}}, \mathbf{X})) \times \text{Prob}(d^{(j)} = -1) \times \text{Prob}(\check{\mathbf{d}}) \times h(\mathbf{X}) \right] dx_1^{(1)} dx_1^{(2)} \cdots dx_1^{(N)} \\ &= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \sum_{\check{\mathbf{d}}} \left[\text{Prob}(y^{(j)} \leq 0 | (d^{(j)} = +1, \check{\mathbf{d}}, \mathbf{X})) \times \text{Prob}(d^{(j)} = +1) \times \text{Prob}(\check{\mathbf{d}}) \times h(\mathbf{X}) \right. \\ &\quad \left. + \text{Prob}(y^{(j)} > 0 | (d^{(j)} = -1, -\check{\mathbf{d}}, \mathbf{X})) \times \text{Prob}(d^{(j)} = -1) \times \text{Prob}(-\check{\mathbf{d}}) \times h(\mathbf{X}) \right] dx_1^{(1)} dx_1^{(2)} \cdots dx_1^{(N)} \\ &= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \frac{1}{2^N} \sum_{\check{\mathbf{d}}} \left[\text{Prob}(y^{(j)} \leq 0 | (d^{(j)} = +1, \check{\mathbf{d}}, \mathbf{X})) + \text{Prob}(y^{(j)} > 0 | (d^{(j)} = -1, -\check{\mathbf{d}}, \mathbf{X})) \right] \\ &\quad \times h(\mathbf{X}) dx_1^{(1)} dx_1^{(2)} \cdots dx_1^{(N)} \end{aligned} \quad (26)$$

$$\begin{aligned} \text{BER}^{(j)} &= \frac{1}{2^{N-1}} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \sum_{\check{\mathbf{d}}} \text{Prob}(y^{(j)} | (d^{(j)} = +1, \check{\mathbf{d}}, \mathbf{X})) \times h(\mathbf{X}) dx_1^{(1)} dx_1^{(2)} \cdots dx_1^{(N)} \\ &= \frac{1}{2^{N-1}} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \sum_{\check{\mathbf{d}}} \frac{1}{2} \text{erfc} \left(\frac{E[y^{(j)} | (d^{(j)} = +1, \check{\mathbf{d}}, \mathbf{X})]}{\sqrt{2 \text{var}[y^{(j)} | (d^{(j)} = +1, \check{\mathbf{d}}, \mathbf{X})]}} \right) \times h(\mathbf{X}) dx_1^{(1)} dx_1^{(2)} \cdots dx_1^{(N)} \end{aligned} \quad (29)$$

$$\begin{aligned} \text{BER}^{(j)} &= \\ &= \frac{1}{2^N} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \sum_{\check{\mathbf{d}}} \text{erfc} \left(\frac{E[y^{(j)} | (d^{(j)} = +1, \check{\mathbf{d}}, \mathbf{X})]}{\sqrt{2 \text{var}[y^{(j)} | (d^{(j)} = +1, \check{\mathbf{d}}, \mathbf{X})]}} \right) \times h_1(x_1^{(1)}) \times h_2(x_1^{(2)}) \cdots \times h_N(x_1^{(N)}) dx_1^{(1)} dx_1^{(2)} \cdots dx_1^{(N)} \end{aligned} \quad (31)$$

Since $x_k^{(j)}$'s, $k = 2, 3, \dots, \beta$, are derived from the iterations of $x_1^{(j)}$, the bit energy depends only on and varies with $x_1^{(j)}$. Define the average bit energy among all bits as

$$\bar{E}_b = \int_{-\infty}^{\infty} \left(\sum_{k=1}^{\beta} (x_k^{(j)})^2 \right) h_j(x_1^{(j)}) dx_1^{(j)}. \quad (35)$$

For a given average bit energy \bar{E}_b , it can be shown that the energy of each bit, given in (34), should be kept independent of $x_1^{(j)}$ in order to optimize the BER in (33). In other words, the bit energy should be kept constant. Suppose the energy is the same for all bits and we denote $\sum_{k=1}^{\beta} (x_k^{(j)})^2$ by E_{cb} . Then, (33) reduces to

$$\begin{aligned} \text{BER}^{(j)} &= \frac{1}{2} \int_{-\infty}^{\infty} \text{erfc} \left(\sqrt{\frac{E_{cb}}{N_0}} \right) h_j(x_1^{(j)}) dx_1^{(j)} \\ &= \frac{1}{2} \text{erfc} \left(\sqrt{\frac{E_{cb}}{N_0}} \right) \end{aligned} \quad (36)$$

which is the optimum BER. In conclusion, to optimize the BER, the following are required.

- 1) The chaotic sequences for different users should have very low correlations even for a finite length; and
- 2) The bit energy should be kept constant for each user.

Application Example: We consider again the use of the Chebychev map for generating chaotic sequences for all users. To provide each user a different chaotic signal, we may either use one Chebyshev map with N different initial conditions or use N Chebyshev maps of different degrees.

Since the initial values $x_1^{(i)}$'s lie between -1 and $+1$, to simplify the mathematics, we substitute $x_1^{(i)} = \cos \phi^{(i)}$ into (31), where $0 < \phi^{(i)} < \pi$ and $\phi^{(m)} \neq \phi^{(n)}$ for $m \neq n$. We write

$$\boldsymbol{\phi} = [\phi^{(1)} \quad \phi^{(2)} \quad \dots \quad \phi^{(N)}]^T \quad (37)$$

for notational clarity. Now, the conditional mean and variance of $y^{(j)}$ can be rewritten as (see Appendix)

$$\begin{aligned} E[y^{(j)} | d^{(j)} = +1, \mathbf{d}, \boldsymbol{\phi}] &= d^{(j)} \sum_{k=1}^{\beta} \left(\cos((M^{(j)})^k \phi^{(j)}) \right)^2 \\ &+ \sum_{i=1, i \neq j}^N d^{(i)} \sum_{k=1}^{\beta} \cos((M^{(i)})^k \phi^{(i)}) \cos((M^{(j)})^k \phi^{(j)}) \end{aligned} \quad (38)$$

and

$$\text{var}[y^{(j)} | d^{(j)} = +1, \mathbf{d}, \boldsymbol{\phi}] = \frac{N_0}{2} \sum_{k=1}^{\beta} \left(\cos((M^{(j)})^k \phi^{(j)}) \right)^2 \quad (39)$$

where $M^{(i)}$ is an integer larger than two and it represents the degree of the Chebyshev map used by the i th user. In general, $M^{(i)}$ can be different for different users. For the case where only one Chebyshev map is used and each user is assigned with a different initial condition, we have the same $M^{(i)}$ value for all i . In either case, $\text{BER}^{(j)}$ is given by (40) at the bottom of the next page. The final result thus consists of 2^{N-1} N -dimensional integrals which we evaluate by the software MATLAB, as implied by the following results.

IV. RESULTS AND EVALUATION

In this section, we evaluate the two aforementioned methods of computing BERs. In particular, we study the following aspects of performance evaluation:

- 1) BER of single-user system;
- 2) BERs of multiuser system with chaotic sequences generated by one Chebychev map with different initial conditions;
- 3) BER of multiuser system with chaotic sequences generated by Chebychev maps of different degrees;
- 4) effect of the number of users on the BER calculations.

$$\begin{aligned} \text{BER}^{(j)} &= \frac{1}{2} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \dots \int_{-\infty}^{\infty} \text{erfc} \left(\frac{\sum_{k=1}^{\beta} (x_k^{(j)})^2}{\sqrt{N_0 \sum_{k=1}^{\beta} (x_k^{(j)})^2}} \right) \times h_1(x_1^{(1)}) \times h_2(x_1^{(2)}) \dots \times h_N(x_1^{(N)}) dx_1^{(1)} dx_1^{(2)} \dots dx_1^{(N)} \\ &= \frac{1}{2} \times \int_{-\infty}^{\infty} h_1(x_1^{(1)}) dx_1^{(1)} \times \int_{-\infty}^{\infty} h_2(x_1^{(2)}) dx_1^{(2)} \times \dots \times \int_{-\infty}^{\infty} h_{j-1}(x_1^{(j-1)}) dx_1^{(j-1)} \\ &\quad \times \int_{-\infty}^{\infty} \text{erfc} \left(\frac{\sum_{k=1}^{\beta} (x_k^{(j)})^2}{\sqrt{N_0 \sum_{k=1}^{\beta} (x_k^{(j)})^2}} \right) h_j(x_1^{(j)}) dx_1^{(j)} \times \int_{-\infty}^{\infty} h_{j+1}(x_1^{(j+1)}) dx_1^{(j+1)} \times \dots \times \int_{-\infty}^{\infty} h_N(x_1^{(N)}) dx_1^{(N)} \\ &= \frac{1}{2} \int_{-\infty}^{\infty} \text{erfc} \left(\sqrt{\frac{\sum_{k=1}^{\beta} (x_k^{(j)})^2}{N_0}} \right) h_j(x_1^{(j)}) dx_1^{(j)} \end{aligned} \quad (33)$$

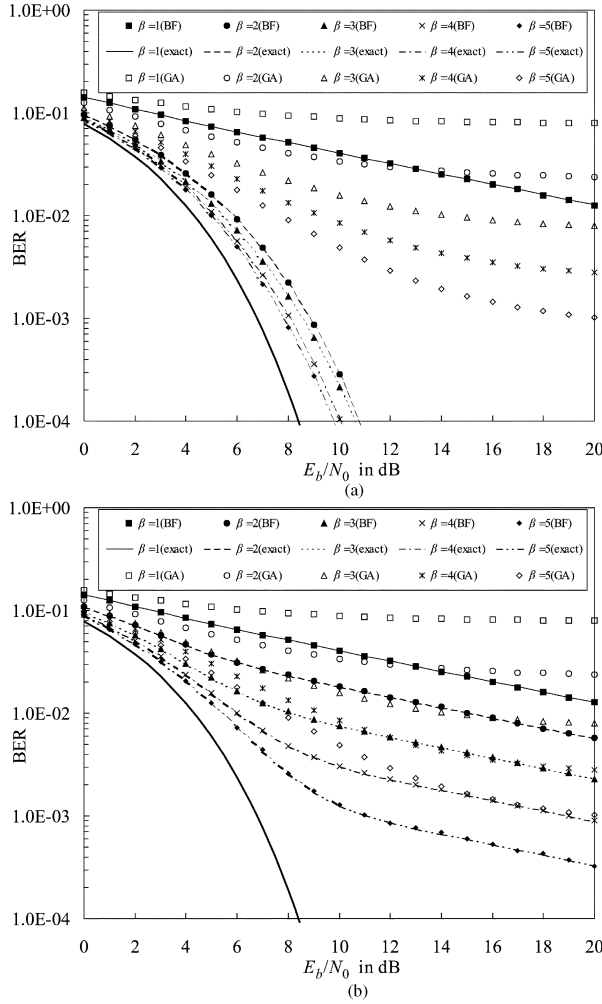


Fig. 2. BERs from the GA-based method, exact analytical method, and BF simulation for a single-user system, with $\beta = 1$ to 5. The optimum BER is plotted as a thick solid curve. (a) Chebyshev map of degree 2 is used as the chaos generator. (b) Chebyshev map of degree 3 is used as the chaos generator.

In each of the first three cases, we compare BERs calculated from the GA-based method and the exact analytical method, with the control data provided by BF numerical simulations. Also, the optimum BER obtained in (36) is plotted for reference. For the last case, we only show the results found from the GA method and BF simulations.

Fig. 2 compares the BERs found from the GA method, the exact method and BF simulations for the single-user CSK

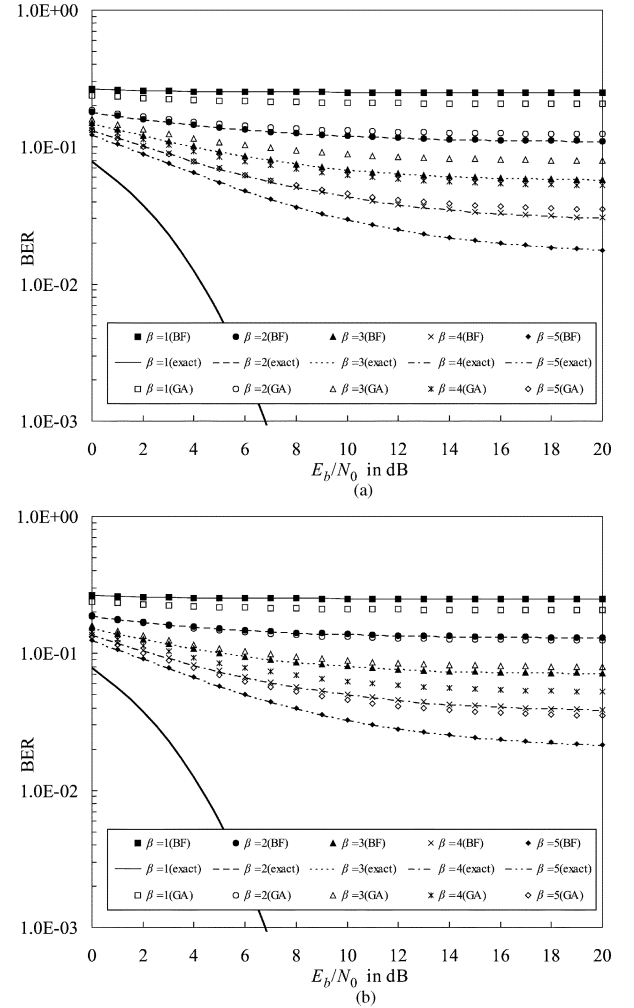


Fig. 3. BERs from the GA-based method, exact analytical method, and BF simulation for a two-user system using one chaos generator with different initial conditions, with $\beta = 1$ to 5. The optimum BER is plotted as a thick solid curve. (a) Chebyshev map of degree 2 is used as the chaos generator. (b) Chebyshev map of degree 3 is used as the chaos generator.

system. Spreading factors varying from 1 to 5 are used, and Chebyshev maps of degrees 2 and 3 are employed as chaos generator (in two separate studies). It is found, because of reliance on low order moments which are the same for all Chebyshev orders, that the BERs obtained by the GA method are the same for both generators, whereas the BERs found from the exact method fully employing the map dynamics show

$$\begin{aligned}
 \text{BER}^{(j)} &= \frac{1}{2^N} \int_{-\pi}^0 \int_{-\pi}^0 \cdots \int_{-\pi}^0 \sum_{\mathbf{d}} \text{erfc} \left(\frac{E[y^{(j)} | (d^{(j)} = +1, \mathbf{d}, \phi)]}{\sqrt{2\text{var}[y^{(j)} | (d^{(j)} = +1, \mathbf{d}, \phi)]}} \right) \frac{1}{\pi \sin(\phi^{(1)})} \times \frac{1}{\pi \sin(\phi^{(2)})} \\
 &\quad \times \cdots \times \frac{1}{\pi \sin(\phi^{(N)})} (-\sin(\phi^{(1)})) (-\sin(\phi^{(2)})) \cdots (-\sin(\phi^{(N)})) d\phi^{(1)} d\phi^{(2)} \cdots d\phi^{(N)} \\
 &= \frac{1}{(2\pi)^N} \int_0^\pi \int_0^\pi \cdots \int_0^\pi \sum_{\mathbf{d}} \text{erfc} \left(\frac{E[y^{(j)} | (d^{(j)} = +1, \mathbf{d}, \phi)]}{\sqrt{2\text{var}[y^{(j)} | (d^{(j)} = +1, \mathbf{d}, \phi)]}} \right) d\phi^{(1)} d\phi^{(2)} \cdots d\phi^{(N)} \quad (40)
 \end{aligned}$$

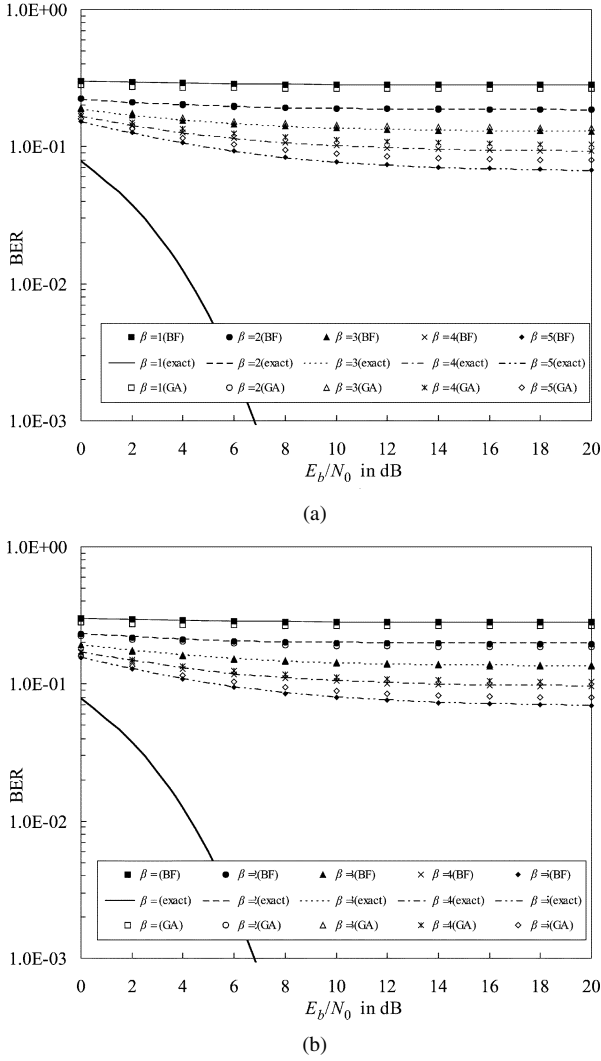


Fig. 4. BERs from the GA-based method, exact analytical method, and BF simulation for a three-user system using one chaos generator with different initial conditions, with $\beta = 1$ to 5. The optimum BER is plotted as a thick solid curve. (a) Chebyshev map of degree 2 is used as the chaos generator. (b) Chebyshev map of degree 3 is used as the chaos generator.

significant difference for the two different chaos generators. Furthermore, the exact method is in perfect agreement with the BF simulations for all cases, whereas the GA method gives deviating results especially for the case where the chaos generator is the Chebychev map of degree 2.

Fig. 3 compares the BERs found from the GA method, the exact method, and BF simulations for the multiuser CSK system employing one chaos generator. Here, we show results for a two-user system for simplicity. Again, spreading factors varying from 1 to 5 are used, and Chebyshev maps of degrees 2 and 3 are employed as chaos generator (in two separate studies). Since one chaos generator is used for the system, two different initial conditions are used to generate chaotic sequences for the two users. Similar observations can be made here. The exact method matches the BF simulations perfectly, whereas the GA methods give deviating results.

When the number of users increases, the approximation by the GA method tends to improve, as shown in Fig. 4 which

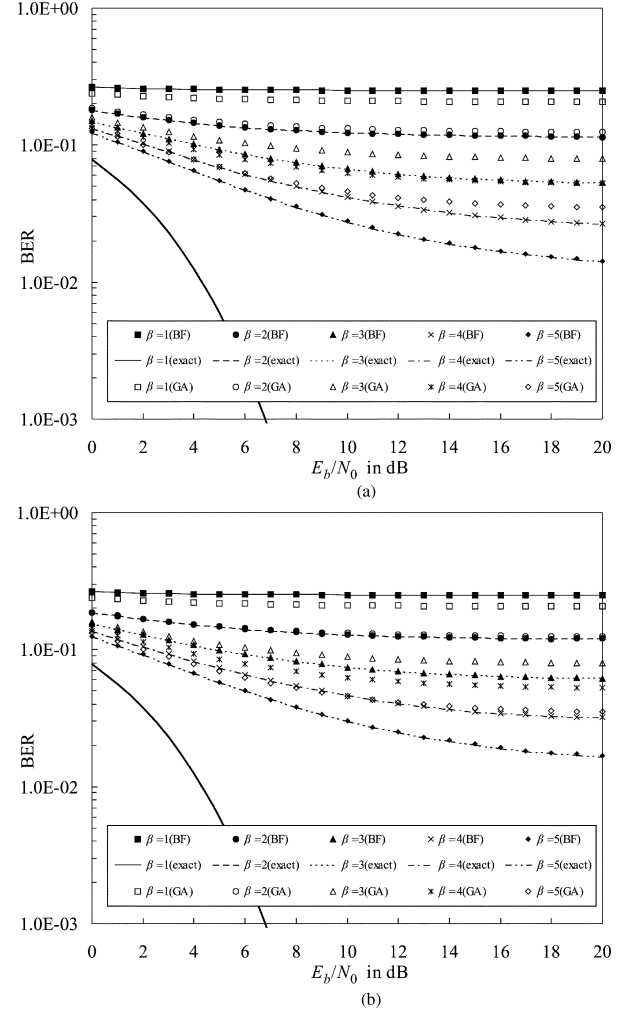


Fig. 5. BERs from the GA-based method, exact analytical method, and BF simulation for a two-user system using two chaos generators for different users, with $\beta = 1$ to 5. The optimum BER is plotted as a thick solid curve. (a) User 1 is using Chebyshev map of degree 2. (b) User 2 is using Chebyshev map of degree 3.

compares the GA method, the exact method and the BF simulations for a three-user system employing one chaos generator. The chaotic sequences for the three users are generated with different initial conditions.

Next, we study the multiuser CSK system employing multiple chaos generators. Here, we show results for a two-user system, in which the Chebychev maps of degrees 2 and 3 are used, respectively, to generate the chaotic sequences for Users 1 and 2. Again, spreading factors of 1 to 5 are used. Fig. 5 compares the results obtained from the GA method, the exact method and the BF simulations. In this case, we observe from the BF simulations that the BERs for the two users are different, due to the use of different chaos generators. The exact method tells this difference, whereas the GA method gives identical results for the two users.

Finally, to show the effect of the number of users on the BER calculations, we plot the BERs against the number of users N for the multiuser system employing one chaos generator. The chaotic sequences for the users are generated with different initial conditions. Fig. 6 shows only the results from the GA

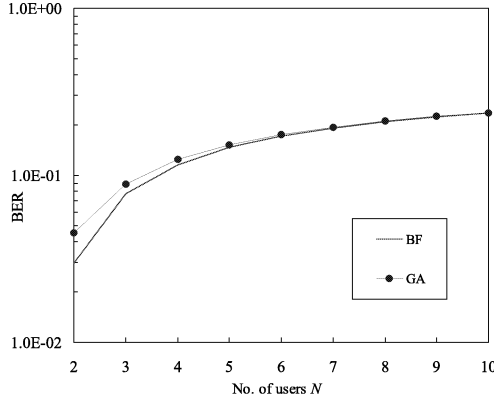


Fig. 6. BERs versus the number of users N from the GA-based method and BF simulation for multiuser system using one chaos generator (Chebyshev map of degree 2) with different initial conditions, at $E_b/N_0 = 10$ dB and $\beta = 5$.

method and the BF simulations for $E_b/N_0 = 10$ dB and $\beta = 5$. Here, the chaos generator is the Chebyshev map of degree 2. It is found that the GA method gives better approximation as the number of users increases. Note that the exact BERs are not plotted in this case. As can be judged from (40), the computational intensity required by the exact method increases exponentially with the number of users N as well as the spreading factor β . Thus, when the number of users or the spreading factor is large, the computational requirement may become too excessive to be feasible; fortunately, this is when the exact results are not required because the GA approximation is sufficiently accurate.

V. CONCLUSION

The process of chaos generation is deterministic. This property allows the prediction of the performance of a chaos-based communication system to be done in an exact manner. In this paper, we have derived an exact analytical expression for a multiuser chaos-shift-keying communication system. Based on the exact analytical expression, it is found that to optimize the BER, the chaotic sequences for different users should have very low correlations even for a finite length, and the bit energy should be kept constant for each user. Because the analytical expression makes no approximating assumption on the distribution of the decision parameter, but note that it is conditionally exactly Gaussian, the exact approach gives totally accurate results compared to the conventional approach of performance evaluation which assumes a Gaussian distributed decision parameter. The exact method will therefore be useful to engineers or researchers, especially those who may not be too familiar with computer simulations, to evaluate and compare the performance of chaos-based communication systems. In this paper, we have shown the application of the method to a particular system. The basic principle is equally applicable to other types of chaos-based communication systems for more performance evaluation. A possible drawback of the exact BER method is that the computational intensity required increases exponentially with the number of users as well as the spreading factor. On the other hand, the work here has verified that this corresponds to increasing accuracy of the GA method.

APPENDIX

STATISTICAL PROPERTIES OF CHAOTIC SEQUENCES GENERATED BY CHEBYSHEV MAP

All symbols are defined as in Section III-A. Consider the Chebyshev map of degree M , defined as [10]

$$g_M(x) = \cos(M \cos^{-1}(x)), \quad -1 \leq x \leq 1. \quad (41)$$

For $M = 2$ and 3, respectively, we have

$$g_2(x) = 2x^2 - 1 \quad (42)$$

$$g_3(x) = 4x^3 - 3x. \quad (43)$$

The invariant probability density function of x , denoted by $\rho(x)$, is [10]

$$\rho(x) = \begin{cases} \frac{1}{\pi\sqrt{1-x^2}}, & \text{if } |x| < 1 \\ 0, & \text{otherwise.} \end{cases} \quad (44)$$

Define

$$\begin{aligned} g_M^{(2)}(x) &= g_M(g_M(x)) \\ g_M^{(3)}(x) &= g_M(g_M^{(2)}(x)) \\ &\vdots \\ g_M^{(k)}(x) &= g_M(g_M^{(k-1)}(x)). \end{aligned} \quad (45)$$

Putting $x = \cos \phi$ in (45), we get, for the case $M = 2$

$$\begin{aligned} g_2(\cos \phi) &= 2 \cos^2 \phi - 1 = \cos 2\phi \\ g_2^{(2)}(\cos \phi) &= g_2(g_2(\cos \phi)) = g_2(\cos 2\phi) \\ &= 2 \cos^2(2\phi) - 1 = \cos(2^2\phi) \\ g_2^{(3)}(\cos \phi) &= g_2(g_2^{(2)}(\cos \phi)) = g_2(\cos(2^2\phi)) \\ &= 2 \cos^2(2^2\phi) - 1 = \cos(2^3\phi) \\ &\vdots \\ g_2^{(k)}(\cos \phi) &= g_2(g_2^{(k-1)}(\cos \phi)) = g_2(\cos(2^{k-1}\phi)) \\ &= 2 \cos^2(2^{k-1}\phi) - 1 = \cos(2^k\phi). \end{aligned} \quad (46)$$

Likewise, we have, for $M = 3$

$$\begin{aligned} g_3(\cos \phi) &= 4 \cos^3 \phi - 3 \cos \phi = \cos 3\phi \\ g_3^{(2)}(\cos \phi) &= g_3(g_3(\cos \phi)) = g_3(\cos 3\phi) \\ &= 4 \cos^3(3\phi) - 3 \cos(3\phi) = \cos(3^2\phi) \\ g_3^{(3)}(\cos \phi) &= g_3(g_3^{(2)}(\cos \phi)) = g_3(\cos(3^2\phi)) \\ &= 4 \cos^3(3^2\phi) - 3 \cos(3^2\phi) = \cos(3^3\phi) \\ &\vdots \\ g_3^{(k)}(\cos \phi) &= g_3(g_3^{(k-1)}(\cos \phi)) = g_3(\cos(3^{k-1}\phi)) \\ &= 4 \cos^3(3^{k-1}\phi) - 3 \cos(3^{k-1}\phi) \\ &= \cos(3^k\phi) \end{aligned} \quad (47)$$

and, in general, we can show that for the Chebyshev map of degree M

$$g_M^{(k)}(\cos \phi) = \cos(M^k\phi). \quad (48)$$

$$\begin{aligned}
E[x_k^2 x_m^2] &= \int_{-\pi}^{\pi} \cos^2 \phi \left(g_M^{(n)}(\cos \phi) \right)^2 \frac{1}{\pi \sin \phi} (-\sin \phi) d\phi \\
&= \frac{1}{\pi} \int_0^{\pi} \cos^2 \phi \left(g_M^{(n)}(\cos \phi) \right)^2 d\phi \\
&= \frac{1}{\pi} \int_0^{\pi} \cos^2 \phi \cos^2(M^n \phi) d\phi \\
&= \frac{1}{\pi} \int_0^{\pi} \left(\frac{1 + \cos 2\phi}{2} \right) \left(\frac{1 + \cos(2M^n \phi)}{2} \right) d\phi \\
&= \frac{1}{4\pi} \int_0^{\pi} \left(1 + \cos 2\phi + \cos(2M^n \phi) + \frac{1}{2} \cos(2(M^n + 1)\phi) + \frac{1}{2} \cos(2(M^n - 1)\phi) \right) d\phi \\
&= \frac{1}{4\pi} \left[\phi + \frac{1}{2} \sin 2\phi + \frac{1}{2M^n} \sin(2M^n \phi) + \frac{1}{4(M^n + 1)} \sin(2(M^n + 1)\phi) + \frac{1}{4(M^n - 1)} \sin(2(M^n - 1)\phi) \right]_0^{\pi} \\
&= \frac{1}{4}
\end{aligned} \tag{52}$$

Moreover, the invariant probability density function of $\cos(\phi)$ can be shown equal to

$$\rho(\cos(\phi)) = \begin{cases} \frac{1}{\pi \sin(\phi)}, & \text{if } 0 \leq \phi \leq \pi \\ 0, & \text{otherwise.} \end{cases} \tag{49}$$

A. Derivation of $\text{cov}[x_k^2, x_m^2]$

First observe that the autocovariance of $\{x_k^2\}$ is

$$\text{cov}[x_k^2, x_m^2] = E[x_k^2 x_m^2] - E[x_k^2]E[x_m^2]. \tag{50}$$

We consider the case where $k \neq m$. Without loss of generality, we assume $m = k + n$ for some positive integer n . Then

$$\begin{aligned}
E[x_k^2 x_m^2] &= \int_{-\infty}^{\infty} x^2 \left(g_M^{(n)}(x) \right)^2 \rho(x) dx \\
&= \int_{-1}^1 x^2 \left(g_M^{(n)}(x) \right)^2 \frac{1}{\pi \sqrt{1-x^2}} dx.
\end{aligned} \tag{51}$$

Using (48) and (49), and $x = \cos \phi$, (51) can be written as (52) shown at the top of the page. Also,

$$E[x_k^2] = \int_{-\infty}^{\infty} x^2 \rho(x) dx = \int_{-1}^1 x^2 \frac{1}{\pi \sqrt{1-x^2}} dx = \frac{1}{2}. \tag{53}$$

Combining (50), (52) and (53), we get

$$\text{cov}[x_k^2, x_m^2] = 0, \quad k \neq m. \tag{54}$$

B. Derivation of $E[x_k x_m]$

The autocorrelation of $\{x_k\}$ is denoted by $E[x_k x_m]$. Consider the case where $k \neq m$ and if we assume $m = k + n$ for some positive integer n , we have

$$\begin{aligned}
E[x_k x_m] &= \int_{-\infty}^{\infty} x g_M^{(n)}(x) \rho(x) dx \\
&= \frac{1}{\pi} \int_0^{\pi} \cos \phi g_M^{(n)}(\cos \phi) d\phi
\end{aligned}$$

$$\begin{aligned}
&= \frac{1}{\pi} \int_0^{\pi} \cos \phi \cos(M^n \phi) d\phi \\
&= \frac{1}{\pi} \int_0^{\pi} \left(\frac{1}{2} \cos((M^n + 1)\phi) + \frac{1}{2} \cos((M^n - 1)\phi) \right) d\phi \\
&= \frac{1}{2\pi} \left[\frac{1}{M^n + 1} \sin((M^n + 1)\phi) + \frac{1}{M^n - 1} \sin((M^n - 1)\phi) \right]_0^{\pi} \\
&= 0.
\end{aligned} \tag{55}$$

REFERENCES

- [1] H. Dedieu, M. P. Kennedy, and M. Hasler, "Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuit," *IEEE Trans. Circuits Syst. I*, vol. 40, pp. 634–642, Oct. 1993.
- [2] M. P. Kennedy, G. Kolumbán, G. Kis, and Z. Jákó, "Recent advances in communicating with chaos," in *Proc. IEEE Int. Symp. Circuits Systems*, Monterey, CA, 1998, pp. 461–464.
- [3] T. Yang and L. O. Chua, "Chaotic digital code-division multiple access communication systems," *Int. J. Bifurc. Chaos*, vol. 7, pp. 2789–2805, 1997.
- [4] Z. Jákó, G. Kis, and G. Kolumbán, "Multiple access capability of the FM-DCSK chaotic communications system," in *Proc. Int. Workshop Nonlinear Dynamical Electronic Systems*, Catania, Italy, 2000, pp. 52–55.
- [5] F. C. M. Lau, M. M. Yip, C. K. Tse, and S. F. Hau, "A multiple access technique for differential chaos shift keying," *IEEE Trans. Circuits Syst. I*, vol. 49, pp. 96–104, Jan. 2002.
- [6] F. C. M. Lau and C. K. Tse, *Chaos-Based Digital Communication Systems: Operation, Analysis and Evaluation*, 1st ed. Heidelberg, Germany: Springer-Verlag, 2003.
- [7] A. J. Lawrance and G. Ohama, "Exact calculation of bit error rates in communication systems with chaotic modulation," *IEEE Trans. Circuits Syst. I*, vol. 50, pp. 1391–1400, Nov. 2003.
- [8] G. Mazzini, G. Setti, and R. & Rovatti, "Chaotic complex spreading sequences for asynchronous DS-CDMA—I: System modeling and results," *IEEE Trans. Circuits Syst. I*, vol. 44, pp. 937–947, Oct. 1997.
- [9] —, "Chaotic complex spreading sequences for asynchronous DS-CDMA—II: Some theoretical performance bounds," *IEEE Trans. Circuits Syst. I*, vol. 45, pp. 496–506, Apr. 1998.
- [10] T. Geisel and V. Fairen, "Statistical properties of chaos in Chebyshev maps," *Phys. Lett.*, vol. 105A, no. 6, pp. 263–266, 1984.